

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

FCC 97-356

RECEIVED
DEC 12 1997
FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of :)
Communications Assistance for) CC Docket No. 97 - 213
Law Enforcement Act)

**COMMENTS OF THE CENTER
FOR DEMOCRACY AND TECHNOLOGY,
THE ELECTRONIC FRONTIER FOUNDATION, and
COMPUTER PROFESSIONALS FOR SOCIAL RESPONSIBILITY**

The Center for Democracy and Technology, the Electronic Frontier Foundation, and Computer Professionals for Social Responsibility respectfully submit these comments on the Commission's Notice of Proposed Rulemaking (NPRM), regarding implementation of Public Law 103-414, commonly referred to as the Communications Assistance for Law Enforcement Act (CALEA).

TABLE OF CONTENTS

I.	Statement of Interest	2
II.	Introduction and Summary of Comments	3
III.	Compliance with CALEA Is Not Reasonably Achievable by the October 1998 Deadline Largely Because the FBI Has Tried to Use the Law to Expand Government Surveillance Capabilities	5
IV.	Carrier Security Policies and Procedures: The Commission Should Not Adopt the Proposed Personnel Security and Recordkeeping Requirements. They Are Beyond the Scope of CALEA. Rather, the Commission Should Focus on Ensuring that Carriers Have Adequate Computer Security Practices to Protect Computerized Surveillance Functions in Central Offices	7

No. of Copies rec'd
List ABCDE

One

A.	Section 105, and the Commission's Rulemaking Authority, Are Limited to the Security of Central Offices	8
B.	Section 105 Was Directed at the Security of Surveillance Activation and Administration Functions within Carrier Central Offices	11
C.	Personnel Security Was Not an Issue in CALEA	14
D.	The Recordkeeping Proposed by the NPRM Does Not Address the Core Concern of Congress in Enacting Section 105, and therefore, the Recordkeeping Provisions Should Not Be Adopted	17
E.	The Commission Should Assure Itself That CALEA Compliance Measures in Central Offices Have Adequate Computer Security Procedures and Practices	18
V.	Congress Adopted for CALEA a Unique Definition of Telecommunications Carrier, Which Is Not Affected by Changes to the Communications Act of 1934	19
A.	The Effect of the 1996 Act	19
B.	Information Services	21
C.	Interexchange Carriers	22
VI.	Conclusion	23
I.	Statement of Interest	

The Center for Democracy and Technology (CDT) is an independent, non-profit, public interest organization in Washington, D.C., working to develop and implement public policies to protect and advance privacy and other democratic values in the new digital communications media. The Electronic Frontier Foundation (EFF) is a non-profit public interest organization devoted to protecting civil liberties and promoting responsibility

in digital media. Computer Professionals for Social Responsibility is a professional society of workers in information industries and people interested in the social impacts of information technologies. In August 1997, CDT and EFF urged the FCC to ensure that implementation of CALEA did not expand law enforcement surveillance capabilities and to enforce CALEA's requirement that carriers protect the privacy and security of communications not authorized to be intercepted.

II. Introduction and Summary of Comments

CALEA is a complicated statute, in which Congress sought to balance three public interests: the law enforcement interest in preserving an electronic communications surveillance capability in the face of changing technology; the industry interest in promoting the timely deployment of innovative services and ensuring fair competition; and the privacy interest in protecting the security and privacy of communications. In requiring telecommunications carriers to design their systems with law enforcement needs in mind, Congress did not want to create new threats to privacy. Therefore, Congress counterbalanced the law enforcement requirements section of CALEA (section 103) with provisions like the systems security provision (section 105) at issue in the NPRM.

The FCC has an important role to play in implementing CALEA. In the NPRM, the Commission has made a good start on some of the key CALEA issues.

However, privacy interests have not been given adequate weight in CALEA implementation, contrary to Congressional intent. We again urge the Commission to exercise its authority under CALEA to protect the telecommunications privacy interests of the American public. The principle of privacy protection is woven throughout CALEA, including in the section on Commission determinations of "reasonable achievability" (section 109(b)(1)). The Commission, in determining what is "reasonably achievable," should reject efforts by the FBI to expand its surveillance capabilities. They are not reasonably achievable in a way that would protect the privacy and security of communications not authorized to be intercepted. To the contrary, some of the punchlist items, by requiring carriers to provide additional information on the signaling channel, would give the government operating under authority of a mere pen register information that it is not authorized to intercept.

The NPRM's proposals regarding carrier security fail to properly discern and fulfill Congress' intent. The Commission's rules should focus not on personnel security and paper recordkeeping requirements, but rather on the computer security measures appropriate to the type of networked surveillance administration systems that carriers will be installing within their central switching facilities as a means of complying with CALEA.

We largely agree with the Commission's interpretation of a key term defined in the law, "telecommunications carrier," and we caution the

Commission against issuance of any rule that would broaden the narrow coverage of CALEA.

III. Compliance with CALEA Is Not Reasonably Achievable by the October 1998 Deadline Largely Because the FBI Has Tried To Use the Law to Expand Government Surveillance Capabilities.

So far, privacy has been the overlooked factor in CALEA implementation, despite Congress' clear directives in the statute.

Under pressure from the Federal Bureau of Investigation (FBI), the industry has adopted an interim standard that would require wireless telephone companies to turn their customers' phones into location tracking devices.

Furthermore, in a decision that has potentially far-reaching implications for the future of telephony, the Internet and government surveillance, the interim standard does not clearly require telecommunications companies using "packet switching" to separate the content of customer communications from the addressing information when the government is only authorized to intercept the addressing data under a pen register or trap and trace authority. Thereby, the standard fails to satisfy the privacy protections of the wiretap laws and fails to comply with CALEA's requirement to "protect the privacy and security of communications ... not authorized to be intercepted." CALEA section 103(a)(4), 47 U.S.C. 1002(a)(4).

Moreover, the FBI is still pushing for additional surveillance features that would go even further beyond preserving the status quo and would

create an even more comprehensive and intrusive government surveillance capability (the so-called "punch-list").

In terms of capacity, the FBI's two inconclusive proposals so far have violated CALEA's requirements and have proposed surveillance capacities far in excess of historical patterns.

Since CALEA was enacted, the FBI has tried to enforce the statute that it originally proposed, rather than the balanced and narrowly-focused statute that Congress enacted. Early versions of digital telephony legislation would have given the Department of Justice design control over the nation's telecommunications system. Congress rejected that approach. It instead enacted broad functional criteria and deferred to the industry standards process to develop solutions, with an appeal to the FCC if that process failed. FBI Director Louis Freeh testified in 1994 that the revised bill was a "remarkable compromise," that it achieved "a delicate, critical balance." He emphasized that the legislation "reflects reasonableness in every provision."¹

Since Congress finished its work, the FBI has rejected reasonableness. It has sought to dominate the industry standards process and has sought to assume for itself the type of design control over the nation's telecommunications system that Congress expressly denied it. The FBI has

¹ Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103rd Cong. (1994) (hereinafter "Hearings") pp. 112-14.

tried to use the statute to exploit the potential of the new digital technology to enhance rather than merely preserve its surveillance capability.

The mandatory enhancement of government surveillance capability and capacity is not what Congress intended in enacting CALEA. The proposals of the FBI are not “reasonably achievable” consistent with the other objectives that Congress sought to balance in CALEA, notably privacy.

IV. Carrier Security Policies and Procedures: The Commission Should Not Adopt the Proposed Personnel Security and Recordkeeping Requirements. They Are Beyond the Scope of CALEA. Rather, the Commission Should Focus on Ensuring that Carriers have Adequate Computer Security Practices to Protect the Computerized Surveillance Functions in Central Offices.

Section 105 is plainly limited to the security of interceptions² effected within a carrier’s switching premises. There is no indication in the text of CALEA or its legislative history that Congress was concerned with the overall security of interception operations when it enacted CALEA. Nor is there any evidence that Congress was concerned with the reliability of carrier personnel. The NPRM is thus flawed in proposing generalized requirements for carrier personnel security and recordkeeping.

Instead, Congress wanted to ensure that CALEA compliance measures adopted within carrier switches would not have the unintended negative side effect of increasing system vulnerability to unauthorized interception. The Commission should assure itself that carriers have appropriate computer

² Throughout these comments, we use the words “surveillance,” “interception,” and “wiretapping” to refer to both interceptions of call content as well as to acquisitions of call-identifying information through pen registers and trap and trace devices.

security plans in place. These plans should include authentication procedures, audit trails, intrusion detection measures, and other standard components of computer security.

Therefore, the Commission's rules should delete the proposed personnel security and recordkeeping measures and instead should focus on procedures for ensuring the security of switch-based surveillance control systems.

A. Section 105 , and the Commission's Rulemaking Authority, Are Limited to the Security of Central Offices.

Section 105 is limited to interceptions "effected within [the] switching premises" of a carrier.³ Section 105 does not cover interceptions effected in a carrier's outside plant (e.g., lines, pedestals, or junction boxes that offer "appearances" where an interception can be effected). Similarly, section 229 refers only to authorized interceptions where carrier officers or employees "activate" the interception; carrier employees do not "activate" outside plant interceptions.⁴

³ Section 105 of CALEA provides:

"SEC. 105. SYSTEMS SECURITY AND INTEGRITY. A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission." (Emphasis added.)

⁴ Section 301 of Pub. L. 103-414 added a new section 229 to title 47, which provides in part:

Contrary to the NPRM, CALEA did not mandate switch-based interceptions.⁵ Under CALEA, carriers are permitted to continue -- as they have in the past -- to assist law enforcement interception merely by providing "cable and pair" information to law enforcement personnel who effectuate the interception themselves in the outside plant without further carrier assistance. This is clearly spelled out in the legislative history:

"This [Section 105] makes clear that government agencies do not have the authority to activate remotely interceptions within the switching premises of telecommunications carrier. Nor may law enforcement enter onto a telecommunications carrier's switching office premises to effect an interception without the carrier's prior knowledge and consent when executing a wiretap under exigent or emergency circumstances under section 2602(c). All executions of court orders or

"(a) IN GENERAL.--The commission shall prescribe such rules as are necessary to implement the requirements of [CALEA].

"(b) SYSTEMS SECURITY AND INTEGRITY.--The rules prescribed pursuant to subsection (a) shall include rules to implement section 105 of [CALEA] that require common carriers--

"(1) to establish appropriate policies and procedures for the supervision and control of its officers and employees --

(A) to require appropriate authorization to activate interception" (Emphasis added.)

⁵ The NPRM incorrectly states that "Section 105 of CALEA requires a telecommunications carrier to enable the interception of communications content or access to call-identifying information via its switching premises." ¶ 21. In fact, section 105 does not impose such a requirement of switch-based interception, nor does any other provision of CALEA. To the contrary, CALEA does not mandate any particular solution. As the Director of the FBI stated in Congressional testimony, "The proposed legislation does not require common carriers to design their systems in any one, particular way." Hearings, *supra* n. 1, p. 31 (prepared statement of FBI Director Freeh). While law enforcement and industry have focused largely on switch-based responses to the four capability requirements of section 103, it is clear that carriers are free to adopt non-switch based solutions. Systems or parts of systems may be able to satisfy the section 103 requirements without going into the switch.

authorizations requiring access to the switching facilities will be made through individuals authorized and designated by the telecommunications carrier. Activation of interception orders or authorizations originating in local loop wiring or cabling can be effected by government personnel or by individuals designated by the telecommunications carrier, depending upon the amount of assistance required." House Rpt. 103-827, Part 1 at p. 26 (emphasis added).

Thus, after CALEA, law enforcement can still activate authorized surveillances in the outside plant or on customer premises without any assistance from carriers, and probably even without the knowledge of carriers.⁶ An outside plant interception is judged only by whether it satisfies the capability assistance requirements of section 103 of CALEA.

Nowhere in the legislative history of CALEA could we find any generalized concern about carrier security practices or about unauthorized wiretapping on carriers' outside plant. The extent to which unauthorized wiretapping occurs on outside plant is debatable, but it is clear that CALEA was not intended to address this problem. Congress had no reason to believe that CALEA would result in changes in the outside plant that might heighten vulnerability and therefore Congress did not impose additional security

⁶ The NPRM is incorrect in stating that "Under CALEA, all interceptions require the intervention and cooperation of a designated and authorized carrier officer or employee." ¶ 21. CALEA does not require a telephone company employee to be present when law enforcement attaches an interception device to the line outside a target's home (or to the telephone or computer inside the target's home). In these dangerous situations, which will be rare but are clearly likely to occur even after CALEA, the telephone company does not want its employees to be present nor would law enforcement want them present. There will be other instances not involving any significant danger (e.g., an interception at a hotel PBX targeted at a particular room), where carrier employees will not be involved, but other persons covered by 18 U.S.C. 2518(4) will be.

requirements on the outside plant. By adding to section 105 the phrase “effected within [a carrier’s] switching premises,” Congress acknowledged that it would always be difficult for carriers to protect millions of miles of wiring and thousands or hundreds of thousands of junction boxes. Therefore, Section 105 imposes no security obligations on carriers with respect to outside plant interceptions.

B. Section 105 Was Directed at the Security of Surveillance Activation and Administration Functions within Carrier Central Offices.

While not mandated, it was generally assumed at the time CALEA was drafted and enacted that many carriers and equipment manufacturers would pursue a switch-based solution to CALEA compliance. It was further assumed that this switch-based solution would involve a software (and perhaps a hardware) upgrade in the computers that increasingly control telecommunications switching.⁷ It was this expectation that CALEA would result in greater reliance on computerized interception within central offices or MTSOs that prompted section 105. Congress felt that if CALEA resulted in carriers’ adopting features in their central switches or MTSOs that made

⁷ “What we are saying is that we have certain requirements with respect to access which they [carriers] tell us are not going into the software, and we want to present those requirements to them, and the statute will compel all of the competitors in this field . . . to put these requirements into their systems as they build the software.” Testimony of FBI Director Freeh, Hearings, *supra* note 1, at p. 10. “If service providers view the electronic surveillance requirements of law enforcement as sophisticated functional ‘features’ there is no reason to believe that the switches (which are essentially specialized computers) cannot accommodate this functionality.” *Id.* at p. 37 (Director Freeh’s Response to Questions Submitted by Senator Pressler).

authorized wiretapping easier, measures should be adopted to ensure that those solutions did not increase system vulnerability.

From the legislative record and other contemporaneous materials, it is clear that Section 105 was intended to address two related concerns: (1) the concern that CALEA compliance measures would allow law enforcement to tap into telephone company switches remotely, and (2) the concern that carriers, in adopting switch-based solutions to CALEA's capability requirements, would adopt features that could be exploited by hackers or others seeking to effectuate interceptions without legal authorization.

1. No remote law enforcement access to switches

At the early stages of the digital telephony debates, there was concern that the legislation would give law enforcement dial-up access to telephone company switches. The New York Times reported on April 19, 1992, "Civil libertarians fear a shift from a world where wiretaps are physically onerous to install . . . to a world where surveillance is so easy that a few pecks on an F.B.I. key pad would result in a tap of anyone's telephone in the country." The Washington director of Computer Professionals for Social Responsibility warned in an opinion piece that "it's clear that the [FBI's] goal is to facilitate remote wiretapping, a type of one-stop shopping for electronic surveillance." ComputerWorld, May 11, 1992. This charge was so volatile that, when the FBI sent its digital telephony proposal to Congress in September 1992, it took care in its section-by-section analysis to make it clear that "The legislation does not establish any independent 'dial-up' authority by which criminal law

enforcement authorities could effectuate interceptions without the affirmative assistance of the providers or operators.” See analysis submitted by letter from Assistant Attorney General Lee Rawls to Speaker Thomas Foley, September 14, 1992, at p. 5. As the drafting process continued, this report language was moved into the legislative language itself, in what ultimately became section 105. Hearings, *supra* note 1, at p. 264 (FBI proposal from 1994). Under section 105, even lawfully authorized interceptions within the carrier’s switching premises cannot be activated remotely by law enforcement.

2. Security within carrier switches

While it was relatively easy to make it clear that CALEA did not give law enforcement the right to activate interceptions remotely, there remained the concern that switch-based interception capabilities were vulnerable to unauthorized manipulation by hackers. In his prepared testimony on April 1994, FBI Director Freeh summarized both the concern and the purpose of section 105:

“Some have raised concerns regarding the impact this legislation might have on network security and reliability. Certain special interest spokespersons have asserted that the legislation will make it easier for anyone, from computer hackers to foreign spies, to access an individual’s communications. These fears are unfounded and misplaced. . . . [T]he proposed legislation includes a “systems security” provision which means that only designated telephone company employees will activate interceptions which originate within telephone company premises.” Hearings, *supra* note 1, at p. 30.

The NPRM does not adequately address the security of intercept functions within the carriers' central offices or MTSOs. As a result of sweeping technological changes in the industry, there is an ongoing convergence of computer and telephone technologies. As the FBI pointed out in its submission to the Judiciary Committees, telephone switches are computers. See note 4, *supra*. In the past, even interceptions within the central office were of an electro-mechanical character, involving the installation of bridges from appearances of copper wires on distribution frames. That technology is disappearing, which was one of the reasons for CALEA.

Under CALEA, it is likely that switch-based wiretap functions will be increasingly computerized. Carriers will establish computerized surveillance administration functions. These functions may be networked with other systems administration functions. They are likely to be linked to functions and locations outside the particular switching office. While law enforcement will not have remote access to these administrative functions, it is likely that carrier employees will. This networking creates a vulnerability, and that is what Congress was worried about.

C. Personnel Security Was Not an Issue in CALEA.

Section 105 should not be turned into a provision for improving the overall security of the telephone system or of interception operations in general. The security of the entire system, including outside plant, was not Congress' concern in CALEA. If it had been, section 105 would not have been

limited to interceptions “effected within [the carrier’s] switching premises.” The FCC’s proposed personnel security requirements are not responsive to the CALEA concerns.

CALEA was not intended to require any generalized changes in carrier practices with respect to the operational security of interceptions. The legislative history of CALEA does not contain any congressional findings or any suggestion in the testimony that existing industry personnel practices were inadequate to protect the integrity of intercept operations. There is no indication that Congress was concerned with the trustworthiness of carrier personnel in general. The focus of Congressional concern was on the vulnerabilities of computerized, switch-based solutions in a networked environment. Therefore, the focus of the FCC rulemaking should be on threats within the central offices.

The NPRM requests comment on whether lists should be compiled of carrier personnel designated to conduct wiretaps and in particular whether law enforcement should be able to obtain from carriers each designated employee’s name and personal identifying information, including date and place of birth and social security number. ¶33.⁸ It is widely assumed that this

⁸ This proposal appears in the section of the NPRM concerning recordkeeping, but we discuss it here under personnel security.

identifying information would be utilized by law enforcement officials to conduct background checks on carrier personnel.⁹

It is unresponsive to Congressional concerns, unnecessary, and unduly intrusive to require personally identifying information to be provided to law enforcement on carrier employees. It is clear from the statutory language and the legislative history that it is carriers who are responsible for selecting, supervising and controlling their own personnel. Section 229 itself provides that the Commission's rules must require carriers "to establish appropriate policies and procedures for the supervision and control of its employees." The NPRM acknowledges that section 229 refers to policies and procedures for supervision of the carrier's own employees. ¶ 25. The legislative history reinforces this point, stating that switch-based interceptions "will be made through individuals authorized and designated by the telecommunications carrier." House Rpt. 103-827, Part 1 at p. 26 (emphasis added). Congress did not intend to give the government supervising control or clearance authority over carrier employees. The Commission should not included the proposed requirement for carriers to make available identifying information on its employees.

⁹ Actually, it is not clear that law enforcement agencies have any authority to conduct background investigations on telephone company personnel who do not receive access to classified information.

D. The Recordkeeping Proposed by the NPRM Does Not Address the Core Concern of Congress in Enacting Section 105, and therefore, the Recordkeeping Provisions Should Not Be Adopted.

Congress wanted carriers to establish mechanisms for preventing unauthorized interceptions in carrier switching facilities. Section 229(b)(2) provides that the rules promulgated by the Commission must require carriers “to maintain secure and accurate records of any interception or access with or without such authorization” (emphasis added). Recordkeeping of the type contemplated by the NPRM does not fully address Congress’ concern. Carrier employees will dutifully create records as they activate authorized interceptions, but they are unlikely to create records on unauthorized interceptions, especially when, as the NPRM notes, the creation of those records is basically admission of a criminal act.

Requiring carriers to keep records of authorized interceptions fails to address the question of identifying unauthorized interception within carrier switches. Reference in section 229(b)(2) to interceptions “with or without authorization” is further evidence that Congress intended carriers to establish some type of audit trails and internal systems monitoring to detect unauthorized interceptions. There are two categories of threats not covered by the NPRM’s record keeping requirements: (1) intentional action by insiders to activate unauthorized interceptions, where the employees involved will simply not fill out the affidavit or record; and (2) intrusions by outsiders. Under the Commission rules, there is no clear indication of how carriers will identify such interceptions. It is these problems that should be addressed.

E. The Commission Should Assure Itself That CALEA Compliance Measures in Central Offices Have Adequate Computer Security Procedures and Practices.

The Commission should focus on the security features that will be associated with the surveillance systems developed by carriers and their equipment manufacturers. This may require a factual inquiry by the Commission, and the consulting of computer security experts. We do not purport in these comments to outline a security program; we can only list some of the factors that should be considered. They include:

- System integrity. The systems (hardware and software) must be tamperproof. Most systems have a maintenance function that allows trapdoor access, which could be used to subvert the system.
- Nontrivial individual authentication. Fixed passwords for user authentication are inherently dangerous, especially when they traverse unencrypted links or reside in system memory, and can be easily captured
- System-to-system authentication. It is likely that the surveillance administration function will be networked with other telephone company systems.
- Audits trails that allow review of surveillance activity.
- Intrusion detection programs that can help identify improper uses.

See generally, Security in Cyberspace, Hearings before the Subcommittee on Investigations of the Senate Committee on Governmental Affairs, June 25, 1996, S. Hrg. 104-701 (testimony of Peter Neumann), pp. 106-111, 350-363, <http://www.csl.sri.com/neumannSenate.html>.

V. Congress Adopted for CALEA a Unique Definition of Telecommunications Carrier, Which Is Not Affected By Changes to the Communications Act of 1934.

A. The Effect of the 1996 Act

We agree with the Commission's tentative conclusion that CALEA's definitions of "telecommunications carrier" and "information services" were not modified by the Telecommunications Act of 1996. We believe that this is correct not only by virtue of Section 601(c)(1) of the 1996 Act, but also because it is clear that Congress intended the definitions of defined terms in CALEA to stand on their own, without being tied to any definitions in the Communications Act, except where specifically noted.¹⁰

One of the most important issues in achieving the CALEA compromise was defining the scope of coverage of the legislation. It is clear that Congress did not want to extend CALEA as broadly as the assistance requirement of 18 U.S.C. 2518(4). It is also clear that for purposes of defining the scope of CALEA coverage, Congress found none of the existing terms in title 18 or title 47 adequate.¹¹ Therefore, for purposes of delineating the coverage of CALEA, Congress adopted unique definitions for "telecommunications carrier" and "information services" suited to the

¹⁰ E.g., CALEA did specifically incorporate by reference the definition of commercial mobile service in the Communications Act.

¹¹ Section 2510 of title 18 already included the term "communications common carrier," which was defined to mean the same thing as the term "common carrier" in the Communications Act. Congress concluded that this term was not appropriate for CALEA purposes, for Congress did not use the term communications common carrier in CALEA.

purposes of CALEA. These definition must be interpreted separately from the definitions of “telecommunications carrier” and “information service” (singular) in the Communications Act of 1934 as amended by the 1996 Act.

Congress made it clear that the definitions of “telecommunications carrier” and “information services” in CALEA were applicable only to CALEA. The definitions section of CALEA begins, “For purposes of this title . . .,” referring to title I of CALEA. And the definitions section of the 1934 Act begins, “For the purposes of this Act,” The definitions section of CALEA did not amend the Communications Act of 1934. Title I of CALEA, while codified in Title 47, is not part of the Communications Act of 1934. Conversely, the definitions section of the 1996 Act amended only the definitions section of the 1943 Act; it did not amend CALEA.

It is a well-established principle of statutory construction that the legislature may develop different definitions of the same or similar terms for use in different contexts. “It is apodictic that Congress may choose to give a single phrase different meanings in different parts of the same statute.” Stowell v. HHS, 3 F.3d 539, 542 (1st Cir. 1993). See also Atlantic Cleaners & Dryers, Inc. v. United States, 286 U.S. 427, 433 (1932). A fortiori, Congress may choose to give different meanings to the same term in different statutes; CALEA and the Communications Act of 1934, as modified by the 1996 Act, are, of course, different statutes.

Also, “it is a ‘basic principle of statutory construction that a statute dealing with a narrow, precise, and specific subject is not submerged by a later

enacted statute covering a more generalized spectrum.” Dalton v. Sherwood Van Lines, 50 F.3d 1014, 1018 (Fed. Cir. 1995) (quoting Radzanower v. Touche Ross & Co., 426 U.S. 148, 153 (1976)). Obviously, the 1996 Act covers a much more generalized spectrum of issues than CALEA.

The conclusion that must be drawn from this is that the definitions of “telecommunications carrier” and “information services” in CALEA are different from the definitions of “telecommunications carrier” and “information service” (singular) in the Communications Act, for reasons separate from section 601 of the 1996 Act.

B. Information Services

The NPRM tentatively concludes that “providers of exclusively information services, such as electronic mail providers and on-line service providers, are excluded from CALEA’s requirements” ¶20. The word “exclusively” does not appear in the statutory definition of information services. The focus of CALEA is on services, not on the exclusive business of the providers. Therefore, information services are exempt even if the companies providing them are engaged in other activities. Indeed, covered telecommunications carriers are exempt from CALEA to the extent they are providing information services. Conversely, any provider of information services is covered by CALEA to the extent that it is providing telephone service as a common carrier for hire. Preserving competitive fairness was one of the objectives of the drafters of CALEA. It would be unfair to cover information services offered by telecommunications carriers but not cover

information services offered by companies not providing telecommunications services. The Commission should be careful in its final rule to avoid any reformulation of the statutory definitions that would cause confusion.

C. Interexchange Carriers

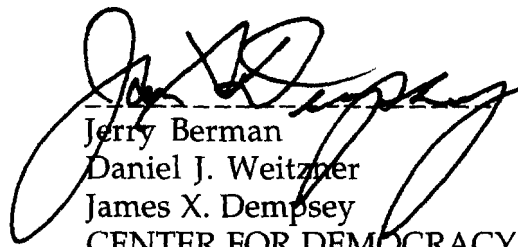
The NPRM proposes including in the rules that may be adopted a list of examples of the types of entities that are subject to CALEA's requirements to the extent that they offer telecommunications services for hire to the public. The proposed list includes "interexchange carriers." ¶ 17. This list is consistent with the legislative history. House Rpt. 103-827, Part 1, at p. 20. However, it should also be noted that CALEA explicitly excludes "equipment, facilities, or services that support the transport or switching of communications for . . . the sole purpose of interconnecting telecommunications carriers." CALEA section 103(b)(2)(B). An important principle in CALEA is that there need not be multiple access points to a communication handled by multiple carriers. See also section 108(a)(1) (carrier cannot be found non-compliant if the facilities of another carrier are reasonably available to law enforcement for implementing the interception). Rather, under CALEA law enforcement must go to the most reasonable access point. As the House report notes, "for communications handled by multiple carriers, a carrier that does not originate or terminate the message, but merely interconnects two other carriers, is not subject to the requirements for the interconnection part of its facilities." House Rpt. 103-827, Part 1, at p. 23.

In order to avoid confusion, it would be better for the Commission to not include the proposed list in its regulations, without restating the other provisions of CALEA affecting interexchange carriers and the other provisions of the legislative history referring to interexchange carriers.

VI. Conclusion

As a result of CALEA, and as a result of technology developments that have computerized telephone switching systems, telecommunications carriers are proposing to establish a computerized surveillance function. In some ways, this function will be more secure than traditional, copper-wire based systems. But in other ways, this function will be more vulnerable. The security measures proposed by the Commission in pursuant of its section 229 responsibilities are inadequate to the task, for they seem to be largely responsive to the pre-digital world. The Commission should shift the focus of the rulemaking to security measures appropriate for a computerized surveillance administration function.

Respectfully submitted,



Jerry Berman
Daniel J. Weitzner
James X. Dempsey
CENTER FOR DEMOCRACY AND
TECHNOLOGY
1634 I Street, N.W.
Washington, D.C. 20006
(202) 637-9800

Stanton McCandlis
ELECTRONIC FRONTIER
FOUNDATION
1550 Bryant Street, Suite 725
San Francisco CA 94103-4832
(415) 436 9333

Andy Oram
COMPUTER PROFESSIONALS FOR
SOCIAL RESPONSIBILITY
P.O. Box 717
Palo Alto, CA 94302
(617) 499-7479
(650) 322-3778

December 12, 1997